North Dakota Homeland Security Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Quick Links

North Dakota

Man charged with terrorizing. A Minot man has been arrested in connection with bomb scare June 4 at a Minot furniture store. The man was charged with terrorizing after he allegedly told other employees of Zimmerman's Furniture that a substance he brought to the store, where he also worked, was C4 plastic explosive. The suspicious substance was removed from the store before the police department's bomb squad removed it from the city and rendered it safe. Source: http://www.minotdailynews.com/page/content.detail/id/540000.html

Regional

(Minnesota) **Nurses' strike ends in Twin Cities.** Thousands of Twin Cities nurses went back to work after a massive one-day strike in Minnesota. Having ramped down operations and hired temporary replacements, some of the 14 affected hospitals said they would only call back their regular nurses as patient volumes required. Late Thursday, both sides claimed to have achieved their goals on a tense and complicated day — the hospitals treating patients with generally little disruption, the union staging a spirited and cohesive walkout that called public attention to their concerns over patient care and nurse staffing levels. No new talks are scheduled, however, leaving each side to weigh the impact of the one-day walkout and consider whether to escalate the dispute. Source: http://www.startribune.com/lifestyle/health/96132824.html?elr=KArks7PYDiaK7DUdcOy_nc:DKUiD3aPc:_Yyc:aU7DYaGEP7vDEh7P:DiUs

(Minnesota) **Northeast Minneapolis blast injures 3.** A "flash explosion" Thursday at a northeast Minneapolis plastics manufacturing plant burned three people, officials said. The blast at Interplastic Corp.'s facility at 2015 NE. Broadway at about 7:30 a.m. seriously injured two workers and left a third needing treatment for minor burns, said a company lawyer. All three were taken to Hennepin County Medical Center, where two were listed in serious condition. The fire department's hazardous-materials unit did an assessment and determined that there was never any health threat to others on the property or to the public. State officials report that Interplastic has been cited several times since 2000 for various environmental problems. The workers were replacing a cap on a 16,000-gallon tank for an acid-based product when the explosion occurred. The ground-level tank was about 20 percent full. "The top blew off, and there was a poof with a brief fire and smoke," read an incident report from the state Department of Public Safety. "The fire burned for 15 seconds." Interplastic makes unsaturated polyester resins, which are flammable and can explode, according to the European Composites Industry Association. Those resins are used for reinforced plastic laminates, electrical components, pipes, tanks and ducts. Source: http://www.startribune.com/local/96062114.html?elr=KArks7PYDiaK7DUdcOy_nc:DKUiD3aPc:_Yyc:aUU

(Montana) **Latvians to be deported for role in Davidson Companies extortion plot.** Three men who aided an extortion plot on Davidson Companies will be deported after receiving their sentence June

10 in Helena, Montana. The three suspects, all of Latvia, previously pleaded guilty to a federal charge of receipt of extortion proceeds. A senior U.S. district judge sentenced the men to time served, as they have been in the custody of Dutch and U.S. officials since February 2008. Conspiracy and extortion charges against the men were dropped in accordance with a plea deal with prosecutors in the U.S. Attorney's Office in Montana. The men were transferred to the custody of the Department of Homeland Security for deportation. Davidson's computer system was hacked into some time between Dec. 20, 2007, and Jan. 11, 2008, by a man identified in court documents as "John Doe, aka [real name]." The hacker has not been arrested and remains at large. Thousands of customers' personal and/or financial account information was accessed as part of the computer attack. The hacker demanded $80,000 from Davidson in exchange for revealing security vulnerabilities and destroying any confidential information he had obtained, court documents state. Source: http://www.greatfallstribune.com/article/20100611/NEWS01/6110321

(Montana) **Bomb squad helps handle volatile chemical.** A Billings, Montana research center was evacuated Tuesday while a bomb squad was called in to handle an unstable chemical found during a routine review. The president of the Billings Clinic Foundation, said the chemical was stored in a laboratory at the research center at 1045 N. 30th St. As part of a regular inventory review, it was discovered that the chemical, picric acid, had changed from a stable liquid into an unstable, crystalline form, which can be explosive. Such deterioration occurs as the water in the acid evaporates over time. A police department bomb squad was called in to safely remove four jars of the acid, which ranged in size up to a half-liter. The bomb squad placed the jars in a containment unit and destroyed them at the landfill. About 18 people evacuated the building while the chemical was removed from the research facility. At the same time, neighboring St. Vincent Healthcare sent out a notice to employees to avoid the area near 11th Avenue North and North 30th Street. The police were notified about the unstable chemical sometime between 10 and 11 a.m., and it was removed from the research center by 3 p.m. Source: http://billingsgazette.com/news/local/article_bd1d0874-7453-11df-93b6-001cc4c03286.html

National

The gulf oil spill: Crisis of unfathomable consequences. On June 4, the Department of Homeland Security Chief and National Incident Commander sent a letter to Congressional leaders warning that the response effort was in danger of running out of money within two weeks and needed cash from the federal oil spill liability trust fund, financed by fees on oil companies. The letter said that as of June 1, federal agencies had already spent $93 million on the spill response, which BP has yet to reimburse. By comparison, in the first quarter of the year, the London-based oil giant's profits averaged $93 million per day. On the same day the officials sent their letter, oil sheen and tar balls arrived with the tide on the Florida panhandle's white sands, including on Pensacola Beach. On June 5, the federal government closed an additional 565 square miles of fishing zones, with the total federal fishery closure now measuring 78,603 square miles, or about 33 percent of the federal waters in the Gulf of Mexico. Source: http://www.worldpress.org/Americas/3566.cfm

New oil plume evidence uncovered. As if the pictures of birds, fish and animals killed by floating oil in the Gulf of Mexico are not disturbing enough, scientists now say they have found evidence of another danger lurking underwater. The University of South Florida recently discovered a second oil plume in the northeastern Gulf. The first plume was found by Mississippi universities in early May. USF has

concluded microscopic oil droplets are forming deep water oil plumes. After a weeklong analysis of water samples, USF scientists found more oil in deeper water. "These hydrocarbons are from depth and not associated with sinking degraded oil but associated with the source of the Deep Horizon well head," said USF Chemical Oceanographer. Through isotopic or microscopic fingerprinting, the USF crew were able to show the oil in the plume came from BP's blown-out oil well. The surface oil's so-called fingerprint matched the tiny underwater droplet's fingerprint. Source: http://www.cnn.com/2010/US/06/07/gulf.oil.plume/

(Ohio; Michigan) **Deadly tornadoes rip through Midwest.** Tornadoes and thunderstorms tore through the Midwest Sunday, killing at least seven people in Ohio and triggering the automatic shutdown of a nuclear power plant in Frenchtown Charter Township, Michigan. In northwest Ohio, seven people were confirmed dead in mostly rural Lake Township south of Toledo. Tornadoes destroyed dozens of homes and heavily damaged the police headquarters and high school, authorities said. Severe storms caused the automatic shutdown of the Fermi 2 nuclear power plant on the shore of Lake Erie in southeast Michigan after a key area of the plant lost its power feed, said a Monroe County spokesman. All safety systems at the plant were functioning and the plant was stable, although an exterior wall was damaged as the siding was ripped off, the spokesman said. Source: http://www.reuters.com/article/idUSTRE6551ZE20100607?type=domesticNews

Coast Guard forms panel for ideas to mop up oil spill. The U.S. Coast Guard is creating a panel to look into proposed technologies and products to clean up the Gulf of Mexico oil spill, concerned that BP Plc's multistage suggestion-box system isn't working. The new group will evaluate ideas that deal with detecting oil in the ocean, cleaning it up and restoring the environment, said a Coast Guard spokesman. The panel will be independent of BP's online efforts to assess ideas. The spill is leaking an estimated 12,000 to 19,000 barrels of oil into the Gulf each day, a government panel said. "There has been a lot of concern that there are significant ideas not getting full voice," the Coast Guard spokesman said in a telephone interview. "The government wanted to make sure that all the best technology is being applied and there was good oversight of that process." The new group will include representatives from the Coast Guard, National Oceanic and Atmospheric Administration, Department of Interior, Environmental Protection Agency and Department of Agriculture. Source: http://www.businessweek.com/news/2010-06-04/coast-guard-forms-panel-for-ideas-to-mop-up-oil-spill-update2-.html

INTERNATIONAL

South Africa terrorism concerns loom as theWorld Cup brackets get under way. June 10, in the article "FIFA World Cup 2010 begins tomorrow amid security concerns," highlighted potential areas of concern, such as IED's and soft targets such as hotels. According toU.S. Navy expert on security issues on the African continent, athletes, and fans who traveling to the 2010 FIFA World Cup soccer tournament must be aware and alert to the fact that a terrorist attack of some kind is a high possibility. Within the last few months, the arrest of al-Qaeda personnel who were planning a terrorist event was confirmation of the threat that exists. The lure of the World Cup for terrorists is "the hundreds of thousands of Western tourists who will pour into South Africa to enjoy tbeaches, game reserves, mountains and the soccer," said the Navy expert. Source: http://www.examiner.com/x-41853-Homeland-Security-Examiner~y2010m6d11-Terrorism-concerns-as-the-World-Cup-brackets-get-under-way

U.S., Europe hit turbulence on ash issue. U.S. and European aviation regulators clashed Tuesday over the hazards of airliners flying through low-level concentrations of ash, with Federal Aviation Administration (FAA) officials reiterating that such plumes should be avoided under nearly all circumstances. Speaking at a safety conference here less than two months after the eruption of an Icelandic volcano temporarily shut down much of Europe's airspace and cost the region's airlines an estimated $1.7 billion in lost revenue, senior regulators from the two sides of the Atlantic laid out dramatically different approaches to the problem. Without directly attacking European decisions to permit flights once ash levels had dropped below a certain limit, FAA policymakers stressed that U.S. safety rules consider even trace volcanic ash potentially as dangerous as violent thunderstorms — and therefore to be avoided if at all possible. The FAA's general counsel and acting deputy administrator, gave an opening speech highlighting the FAA's policy of staying out of day-to-day decisions about authorizing flights. "We did not want to convey the impression that somehow we knew how to do things better than" European regulators, the official said. The FAA, he told the conference, remains convinced the correct option is to tell pilots to avoid ash, provide them with the best possible forecasts and then let individual airlines "make the fly or no-fly decisions." Carriers are "better able to integrate the risks" than government bureaucrats, he said, and Europe's efforts amounted to a "different response from what we would have done." Source: http://online.wsj.com/article/SB10001424052748704256604575295430533564348.html?mod=WSJhpp_MIDDLENexttoWhatsNewsTop

Banking and Finance Industry

SEC eyes confluence of events as flash crash cause. U.S. regulators will most likely find that a confluence of events caused the unprecedented stock market "flash crash" in early May, the Securities and Exchange Commission (SEC) chairman said June 10. For a month, regulators have been trying to determine what caused the Dow Jones Industrial Average to plunge some 700 points in minutes May 6 before sharply rebounding. Earlier June 10, the SEC approved a mechanism to temporarily pause trading in single stocks when markets are plunging uncontrollably. The stock-specific circuit breakers, being adopted this month, will halt trading for five minutes in any S&P 500 share if it falls more than 10 percent in five minutes. The chairman said she was anxious to expand the stock-specific mechanism to other stocks and to a number of exchange-traded funds, which were hit harder than ordinary stocks in the brief market freefall. Source: http://in.reuters.com/article/idINIndia-49217820100611

Skimming from the sofa. Skimming devices attached to cash machines to read users' card details increasingly return their data to the criminals via SMS text messages. The devices copy the magnetic strip of cash point and credit cards at the card slot and spy on PINs via keyboard attachments or mini cameras. The data is subsequently used by the skimmers to withdraw money from users' accounts. More details on this method of attack can be found in The H Security article "Manipulated ATMs - Attack of the card cloners." The new generation of skimming devices no longer store the data over a period of time for later collection, but transmit it via SMS directly to the criminals, allowing them to clone card details from the comfort of their own living room. The risk of getting caught is reduced by 50 percent because criminals no longer need to retrieve the skimming device to read out the data. The only time a perpetrator needs to go to the cash machine is to mount the device. This method isn't entirely new, of course, as some skimming devices have transmitted their data via short-distance

radio for quite a while. However, with a radio link, the criminals need to keep their receivers within range of the device. Source: http://www.h-online.com/security/news/item/Skimming-from-the-sofa-1016534.html

Domestic microfinance steps into the credit breach. During the credit crunch, small business owners rejected by traditional lenders found growth funding through domestic microfinance organizations geared to helping the poor and disenfranchised. Loan applications have increased in the past two years at 66 percent of microfinance groups surveyed by the Aspen Institute, a policy and research organization. While only a few microlenders were able to accommodate a majority of new applicants, those more likely to get funding were "people who were very strong small business owners who in the past would have received financing, but because the banks pretty much shut down, they did not," said the director of Aspen's microenterprise FIELD project, which tracks domestic microfinance and conducted the survey. Domestic microfinance will never replace traditional business lending, nor should the industry drop its primary goals of social improvement and poverty alleviation, said a venture capitalist and professor of microfinance at the University of California, Berkeley. The industry, which reported lending an aggregate $68.6 million in FIELD's survey from financial year 2008, represents only a drop in the bucket of the U.S. credit market. But it is growing fast and has taken on new importance during the recession. Source: http://www.businessweek.com/smallbiz/content/jun2010/sb2010064_156475.htm

Three banks closed on June 4. Federal and state banking regulators closed three banks June 4, raising the number of failed institutions to 89 so far in 2010. First National Bank, Rosedale, Miss., was closed by the Office of the Comptroller of the Currency, which appointed the Federal Deposit Insurance Corp. (FDIC) as receiver. The FDIC entered into a purchase and assumption agreement with The Jefferson Bank, Fayette, Mississippi, to assume all deposits of First National Bank. The FDIC estimates that the cost to the Deposit Insurance Fund (DIF) will be $12.6 million. The FDIC approved the payout of the insured deposits of Arcola Homestead Savings Bank, Arcola, Illinois. The bank was closed by the Illinois Department of Financial Professional Regulation - Division of Banking, which appointed the FDIC as receiver. The FDIC estimates that the cost to the DIF will be $3.2 million. TierOne Bank, Lincoln, Neb., was closed by the Office of Thrift Supervision, which appointed the FDIC as receiver. The FDIC entered into a purchase and assumption agreement with Great Western Bank, Sioux Falls, South Dakota, to assume all of the deposits of TierOne Bank. The FDIC estimates that the cost to the DIF will be $297.8 million. Source: http://www.bankinfosecurity.com/articles.php?art_id=2612

Chemical and Hazardous Materials Sector

Nothing Significant to Report

Commercial Facilities

(Arkansas) **Osage Baptist Church bomb blown upby Bentonville bomb squad.** Members of the Bentonville, Arkansas bomb squad bleup what they believe was bomb found inside the Osage Baptist Church June 9. The device was found in the foyer of the church. It had been moved to the gravel parking when a Carroll County deputy arrived. Once the bomb squad arrived, X-rays of the device revealed it contained electronic devices. A water cannon blew the device apartBomb technicians classified the device as an improvised explosive device. The churchad been a polling place June 8 for

Arkansas' runoff elections. Source:
http://www.todaysthv.com/news/local/story.aspx?storyid=106346&catid=2

(Maryland) **Montgomery County Police searching for copper pipe thief.** Montgomery County, Maryland Police are investigating a series of copper pipe thefts occurring throughout the county in the month of May. Detectives saod that the copper pipes and downspouts were forcefullyremoved from the side of buildings and taken away. A total of eight buildings were e. n a are he w lot . h targeted, most of them churches. The thefts are believed to have occurred in the evening or overnight hours between 8 p.m. and 8 a.m. Police believe the suspect may be selling the copper items to area scrap yards for thousands of dollars. Detectives have obtained surveillance video of the suspect carrying downspouts that he had just pulled off the United Church of Christ in Bethesda. The suspect is described as a white male, 5'9" to 6'1" tall, 180 to 190 pounds, with brown or black hair. The suspect was wearing a blue T-shirt, blue jeans and black boots. Source:
http://www.myfoxdc.com/dpp/news/maryland/montgomery-county-police-searching-for-copper-pipe-thief-061010

(North Carolina) **Bomb threat evacuates Durham hotel.** Police responded to a bomb threat at the Crestwood Suites Hotel in Durham, N.C. June 9. It happened around 7:45 p.m. on Meredith Drive near the intersection of highways 54 and 55. Police received a call that there was a bomb in a room at the hotel. All of the guests were forced out of their rooms and police limited traffic in and out of the property. Authorities have made an arrest, but they have not released the person's name or any other information about the incident. Source:
http://abclocal.go.com/wtvd/story?section=news/local&id=7488787

Jihadi calls for 'suspicious bags' to be left throughout DC and NYC. A recent internal FBI report warns federal, state, and local authorities to be alert for a potential new tool in the jihad terror arsenal – the placing of suspicious, but harmless, bags in public places to inspire fear, disrupt public transportation, and tie up police and bomb squads. The so called "battle of suspicious bags" was encouraged by an unknown poster to a known jihadi Web site. On May 12, the poster suggested an "invasions suspicious bags (sic)" in "the heart of Washington D.C. and New York." The bags would contain not bombs, but innocuous items, a tactic that has been used by other political extremists in the U.S. in the recent past. "The stated goal of the campaign," said the report, "was to exploit desensitization of first responders caused by response fatigue to suspicious, but harmless items." The FBI report did not include the full text of the jihadi forum post. The poster's credibility was not known, but the site where the information was posted was listed as a "known jihadi Web site." Source:
http://abcnews.go.com/Blotter/jihadi-calls-suspicious-bags-left-dc-nyc/story?id=10826590

Communications Sector

(Iowa) **Hinton explosion causes cell tower disruption.** Verizon Wireless is working on a temporary cell phone tower after an explosion June 9 destroyed a building next to an existing tower, a local fire official said. The Hinton fire chief said the explosion was reported about 8:30 p.m. in a small building at the base of a cell phone tower near Hinton. Although the blast didn't damage the actual tower, he said it destroyed the building and required the tower be turned off. The temporary structure was expected to be in place on June 10 or early June 11. A leaking propane tank from a backup generator allowed gas to fill the small building, which blew up when a spark ignited the flammable gas. Source:

http://www.siouxcityjournal.com/news/local/crime-and-courts/article_e6094d28-74ef-11df-8ac2-001cc4c03286.html

AT&T: Security gap exposed Apple iPad e-mail addresses, IDs. AT&T said late June 9 that a security breach had exposed the e-mail addresses of Apple iPad users. The nation's second-largest wireless service provider said that the problem had been fixed and that it would inform customers of the breach, which also exposed their iPad identification numbers used to authenticate a wireless user. Gawker reported that the information was obtained by a hacker group calling itself Goatse Security. The group used a script on AT&T's Web site, accessible to anyone on the Internet, to get the data. The hacker group obtained the e-mail addresses of top-level politicians, television reporters and business executives, including the White House chief of staff. AT&T did not say how many customers were affected. But Gawker, which reported the breach June 9, said 114,000 e-mail addresses were exposed. Apple, which says it has sold 2 million iPads since it was launched last April, did not immediately respond to an interview request. "The issue has escalated to the highest levels of the company and was corrected by [June 8]; and we have essentially turned off the feature that provided the e-mail addresses," AT&T said in a statement. Source: http://voices.washingtonpost.com/posttech/2010/06/att_says_security_hole_exposed.html?hpid=topnews

First responders launch campaign for nationwide communications network. "The unprecedented unity in the first-responder community demonstrates how critical this communications capability is for those who put their lives on the line everyday to protect America," the San Jose Chief of Police and Major Cities Chiefs Association President said. "Almost nine years since this need was tragically underscored on 9/11, it's long overdue for Congress immediately to hold hearings and help keep America safe by providing this nationwide communications network, controlled and operated by public safety, not by commercial carriers." Specifically, the Federal Communication Commission's (FCC) National Broadband Plan calls for the auction of the 700 MHz D-Block spectrum to wireless carriers for commercial use. Public safety and numerous industry experts view the FCC's plan for commercial carriers to build, implement and operate the system as technically, competitively and operationally flawed. The Public Safety Alliance is calling for Congressional hearings and for Congress to allocate the D-Block spectrum to public safety. The Public Safety Alliance supports H.R. 5081, the Broadband for First Responders Act of 2010, which would allocate directly to public safety the spectrum needed to establish a nationwide interoperable communications network. Source: http://www.prweb.com/releases/2010/06/prweb4099274.htm

Defense Industrial Base Sector

Lockheed Martin F-35 ground-test article completes testing five months ahead of schedule. F-35 Lightning II program successfully completed F-35A conventional takeoff and landing (CTOL) full-scale static testing – with zero structural failures – five months ahead of schedule, and in less than half the time of legacy programs. The test program was conducted on AG-1, an F-35A dedicated to validating the strength of the jet's airframe. During testing, the strength and stability of the aircraft structure were verified to 150 percent of design limits or 13.5 G's, with 174 critical-load conditions, or pressures, applied to the airframe to evaluate its structural integrity. Testing was conducted predominantly in Brough, England. The U.K. tests began in August 2009 and were accomplished in 295 days – a rate that exceeded the record-setting pace previously established by the F-35B short

takeoff/vertical landing static test program. The managing director for the F-35 program said: "This was a major milestone, and the test results demonstrate that the F-35 has a fantastic airframe." Source: http://www.prnewswire.com/news-releases/lockheed-martin-f-35-ground-test-article-completes-testing-five-months-ahead-of-schedule-95982819.html

American citizen from Maryland and five Iranians indicted in conspiracy to illegally provide satellite technology to Iran. A federal grand jury has indicted six individuals, one American and five Iranian citizens, on charges of conspiring to illegally provide satellite hardware and technology to Iran, in violation of the International Emergency Economic Powers Act and money laundering. The indictment alleges that as a result of the conspiracy, an Iranian earth satellite equipped with a camera was launched into space in Russia on Oct. 27, 2005. The indictment was returned June 2 and unsealed June 8. A 49-year-old Potomac, Maryland resident, who is a naturalized U.S. citizen born in Iran, was arrested. The five Iranian-citizen defendants remain at large. Source: http://www.prnewswire.com/news-releases/american-citizen-from-maryland-and-five-iranians-indicted-in-conspiracy-to-illegally-provide-satellite-technology-to-iran-95878974.html

(California) **Air Force tests missile interceptor.** The Air Force said it successfully launched a missile interceptor rocket from California for test purposes. The ground-based interceptor was launched at 3:25 p.m. June 6 from Vandenberg Air Force Base. The Air Force said it was a flight test of a two-stage variant of the operational three-stage interceptors deployed at the Central coast base 130 miles northwest of Los Angeles. The mission did not involve a launch of a target missile. Source: http://www.militarytimes.com/news/2010/06/ap_missile_interceptor_060710/

(Florida) **Falcon 9 soars on debut flight.** Overcoming a main engine abort, a Flight Termination System communications glitch and a boat that strayed into the launch danger zone, Space Exploration Technologies (SpaceX) successfully launched its debut Falcon 9 rocket Friday afternoon on a test flight prior to a demonstration mission for NASA this summer. Rising from a refurbished Titan launch complex at Cape Canaveral Air Force Station in Florida, the 48-meter tall booster blasted off and achieved an orbit 250 km. (160 mi.) above the Earth and inclined 34.5 deg. The only obvious blemish on the mission was an apparent parachute failure on the rocket's recoverable first stage, which caused it to slam into the Atlantic and break apart The SpaceX team recovered from a previous launch attempt earlier in the afternoon when one of the rocket's nine first-stage motors triggered an automated abort a few seconds before liftoff. Engineers also had to overcome a telemetry problem with the Falcon 9's Flight Termination System to assure that the 45th Space Wing's Range Safety Office was getting a good signal. A third delay was due to boat straying into the launch danger zone. Nine minutes and 38 seconds after launch, the Falcon 9's payload — a mockup of SpaceX's Dragon capsule — was in orbit. Source: http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=space&id=news/awx/2010/06/04/awx_06_04_2010_p0-232127.xml

Laser system goes 2-for-2 in key test. One of the Navy's first laser weapons got a step closer to the fleet's arsenal in late May when engineers proved it could find, track and zap targets over the ocean in a test firing off the West Coast. Dubbed the Laser Weapons System, or LaWS, the weapon destroyed two drones in what sailors would know as a detect-to-engage exercise, partly using familiar sensors already on scores of ships in the fleet as part of their Phalanx Close-In Weapons Systems. Navy engineers hope LaWS will join CIWS on ships in the next six or seven years to become the new

go-to safeguard against fast, dangerous anti-ship missiles. A laser CIWS would give a ship more accuracy and a theoretically infinite magazine, compared with the smothering but still limited ordnance of today's Gatling gun version. LaWS, which was on land, zapped both drones May 24 in a test at San Nicholas Island, California — its first firing over the ocean. In a test last year, the laser destroyed all five unmanned targets at White Sands Missile Range, New Mexico, but that was in a clear, dry desert environment. Moisture in the atmosphere can disrupt directed energy weapons, which is a central challenge in fielding them aboard ships. Source: http://www.militarytimes.com/news/2010/06/navy_lasers_060510w/

Critical Manufacturing

GE recalls front-loading washing machines. GE is recalling about 180,000 front-load washing machines. A wire can break in the machine and make contact with a metal part on the washtub while the machine is operating, posing fire and shock hazards to consumers. GE is aware of seven incidents in which flames escaped the units and caused minor smoke damage. No injuries have been reported. This recall involves GE front-load washing machines without auxiliary water heating. Recalled washing machines were manufactured between December 2006 and February 2010. The model and serial numbers are located on the bottom right side and on the bottom door frame of the washers. The washing machines, made in China, were sold at department and various retail stores nationwide from December 2006 through May 2010 for about $700. Consumers should immediately stop using the recalled washers, unplug it from the electrical outlet and contact GE for a free repair. Consumers should not operate the washer until it has been repaired. Source: http://www.consumeraffairs.com/recalls04/2010/ge_washers.html

GM recalling 1.5M vehicles over fire concerns. General Motors said Tuesday it was recalling about 1.5 million vehicles worldwide to address a problem with a heated windshield wiper fluid system that could lead to a fire, its second recall over the issue in two years. The recall affects several pickup trucks, sport utility vehicles, crossovers and passenger car models from the 2006 to 2009 model years. GM conducted a similar recall in 2008 but came across new reports of fires in vehicles that had been fixed. GM said it would disable the heated washer fluid system module that could lead to fires. The Detroit automaker will pay owners and those leasing vehicles $100 each since the feature is being disabled. GM said it was aware of five fires but there had been no injuries or crashes reported. Nearly 1.4 million vehicles are in the U.S. and more than 100,000 vehicles are in Canada, Mexico and other international markets. Source: http://wtop.com/?nid=25&sid=1975323

(Florida) **Falcon 9 soars on debut flight.** Overcoming a main engine abort, a Flight Termination System communications glitch and a boat that strayed into the launch danger zone, Space Exploration Technologies (SpaceX) successfully launched its debut Falcon 9 rocket Friday afternoon on a test flight prior to a demonstration mission for NASA this summer. Rising from a refurbished Titan launch complex at Cape Canaveral Air Force Station in Florida, the 48-meter tall booster blasted off and achieved an orbit 250 km. (160 mi.) above the Earth and inclined 34.5 deg. The only obvious blemish on the mission was an apparent parachute failure on the rocket's recoverable first stage, which caused it to slam into the Atlantic and break apart The SpaceX team recovered from a previous launch attempt earlier in the afternoon when one of the rocket's nine first-stage motors triggered an automated abort a few seconds before liftoff. Engineers also had to overcome a telemetry problem with the Falcon 9's Flight Termination System to assure that the 45th Space Wing's Range Safety

Office was getting a good signal. A third delay was due to boat straying into the launch danger zone. Nine minutes and 38 seconds after launch, the Falcon 9's payload — a mockup of SpaceX's Dragon capsule — was in orbit. Source: http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=space&id=news/awx/2010/06/04/awx_06_04_2010_p0-232127.xml

Emergency Services

Mechanical problems hampered Coast Guard rescue after Gulf rig blast. Serious mechanical problems with Coast Guard aircraft and vessels delayed, cut short or aborted rescue efforts after the Deepwater Horizon drilling rig exploded in the Gulf of Mexico April 20, according to an investigation by the Center for Public Integrity. Logs show the Coast Guard "averaged one problem for every seven rescue sorties it operated during the first three days of the oil spill crisis in April," the investigation found. In one instance, 38 minutes were lost trying to evacuate workers from the burning rig or rescue those who jumped into the water because the crew of a 25-year-old helicopter had to switch to another aircraft. Similar mechanicals problems plagued rescue efforts after the Haiti earthquake in January. A Coast Guard official said the problems "were nothing that was not out of the ordinary." Source: http://content.usatoday.com/communities/ondeadline/post/2010/06/mechanical-problems-hampered-coast-guard-resuce-after-gulf-rig-blast/1

(California) **Vintage military rocket aimed at Calif. station.** Hemet, California, police said Tuesday that a vintage military training rocket was ignited and aimed at the Hemet police station last week, in what detectives are treating as an incident related to five previous attacks on officers. The model-M29A2 rocket, described among military enthusiasts as a shoulder-fired bazooka missile used in World War II, was found on the roof of the Los Altos Market on North Carmalita Street, shortly after 10 p.m. Thursday, a Hemet police lieutenant said. Because the rocket was pointed diagonally across the street from the Hemet police station, authorities believe the rocket is the latest in a string of attacks on Hemet police and the city since New Year's Eve. The description of the rocket was released Tuesday. During the days immediately after a fire that burned several wooden pallets behind the market, police said only that a suspicious device had been found at the scene. Hemet firefighters found the 9-pound rocket, with its motor ignited, indicating an attempt was made to fire it, while responding late Thursday to the fire. They reported it to police and the Riverside County sheriff's Hazardous Device Team. Detectives are investigating what caused the fire. No one was injured in the fire or by the rocket. Source: http://www.officer.com/online/article.jsp?siteSection=1&id=52816

Energy

Baker Hughes: U.S. oil, gas rig count down 29 to 1,506 this week. The number of rigs drilling for oil and natural gas declined this week as the growing oil spill in the Gulf of Mexico and subsequent drilling ban pared back activity. The number of oil and gas rigs fell to 1,506 rigs, down 29 from the previous week, according to data from oil-field services company Baker Hughes Inc. The number of gas rigs was 947, a decrease of 20 from last week, while the oil rig count was 545, a decrease of 10 rigs. The number of miscellaneous rigs rose by one to 14 rigs. A drilling ban in the Gulf of Mexico that was imposed as a result of the oil spill prompted the drop-off in drilling activity. Oil is still spewing from the damaged BP PLC well in the Gulf following an April 20 explosion aboard a Transocean Ltd.

rig. The offshore drilling rig count fell by half this week to 24 rigs, according to Baker Hughes. Source: http://online.wsj.com/article/BT-CO-20100604-709915.html?mod=WSJ_latestheadlines

Food and Agriculture

USDA: Erosion down, farmland losses up. About 40 million acres of land were newly developed between 1982 and 2007, bringing the national total to about 111 million acres. More development occurred in the Southeast than in any other region. The National Resource Inventory (NRI) definition of developed land includes rural transportation corridors such as roads and railroads, as well as residential, industrial, commercial and other land uses. Soil erosion on cropland declined by more than 40 percent over the past 25 years, but more than one-third of development of U.S. land occurred during the same period. That's according to the latest NRI Inventory for non-federal lands by the U.S. Department of Agriculture's Natural Resources Conservation Service. Total cropland erosion dropped by 43 percent, from more than 3 billion tons per year in 1982 to 1.72 billion tons annually in 2007. Most of the erosion reductions occurred between 1987 and 1997. Cropland acreage declined 15 percent from 420 million acres in 1982 to 357 million acres in 2007. About half of that reduction is reflected in enrollments of environmentally sensitive cropland in USDA's Conservation Reserve Program. Source: http://southeastfarmpress.com/news/erosion-down-farmland-losses-up-0611/

EPA moves to terminate all uses of insecticide endosulfan to protect health of farmworkers and wildlife. The U.S. Environmental Protection Agency (EPA) is taking action to end all uses of the insecticide endosulfan in the United States. Endosulfan, which is used on vegetables, fruits, and cotton, can pose unacceptable neurological and reproductive risks to farmworkers and wildlife, and can persist in the environment. New data generated in response to the agency's 2002 decision have shown that risks faced by workers are greater than previously known. EPA also finds that there are risks above the agency's level of concern to aquatic and terrestrial wildlife, as well as to birds and mammals that consume aquatic prey which have ingested endosulfan. Farmworkers can be exposed to endosulfan through inhalation and contact with the skin. Endosulfan is used on a very small percentage of the U.S. food supply and does not present a risk to human health from dietary exposure. Makhteshim Agan of North America, the manufacturer of endosulfan, is in discussions with EPA to voluntarily terminate all endosulfan uses. EPA is currently working out the details of the decision that will eliminate all endosulfan uses, while incorporating consideration of the needs for growers to timely move to lower-risk pest-control practices. Endosulfan, an organochlorine insecticide first registered in the 1950s, also is used on ornamental shrubs, trees, and herbaceous plants. It has no residential uses. Source: http://yosemite.epa.gov/opa/admpress.nsf/0/44C035D59D5E6D8F8525773C0072F26B

USDA permits planting of genetically modified trees. South Carolina-based biotechnology company, Arbor Gen, has received approval from the U.S. Department of Agriculture (USDA) to move ahead with plans to plant genetically-modified eucalyptus trees in seven southern states. Arbor Gen has modified the trees so they could grow further north in colder areas. USDA has granted permission to plant up to 250,000 of thetrees on 28 sites in Florida, South Carolina, Georgia, Alabama, Mississippi, Louisiana and Texas. The fast-growing trees would be used for pulp to make paper. Opponents say eucalyptus trees use a lot of water and are already an invasive species, and that genetic modification only adds to that threat. The USDA permits are for experimental planting only; any commercial

production would require additional permits. Source: http://www.truthabouttrade.org/news/latest-news/16098-usda-permits-planting-of-genetically-modified-trees

U.S. to study honeybee populations. The federal government is embarking on its most ambitious survey ever of honeybee pests and diseases 13 states. The national survey follows decades of steep losses of honeybees — a trend sharply accentuated by the onset in 2006 of Colony Collapse Disorder, characterized by adult bees leaving the hive and never returning. The survey will look at 350 apiaries, or a collection of honeybee colonies, across 13 states through the end of this year. It is being conducted by USDA's Animal and Plant Health Inspection Service and Agricultural Research Service and by Penn State University. Survey kits have been mailed to state apiary specialists, who will collect samples of bees and debris from apiaries in their states. The survey is funded for just one year but will have to continue for at least three or four more years to produce meaningful results. The survey will take place in Alabama, California, Georgia, Indiana, Florida, Hawaii, Michigan, New York, Pennsylvania, South Dakota, Tennessee, Texas, and Washington. Source: http://www.pittsburghlive.com/x/pittsburghtrib/news/s_685108.html

Report says FDA struggles to keep food safe. A new report says the Food and Drug Administration (FDA) is stretched thin and needs to reorganize to better keep the nation's food safe. The report released by the Institute of Medicine and the National Research Council Tuesday said the agency needs to become more efficient and better target its limited dollars to prevent food-borne illness outbreaks. The chairman of the committee that authored the report, said the FDA is too often reactive and not focused enough on prevention. The report recommends the agency focus on preventing outbreaks in the riskiest foods rather than tackling problems on a case-by-case basis. The FDA is responsible for ensuring the safety of about 80 percent of the nation's food supply. Source: http://www.ksn.com/news/national/story/Report-says-FDA-struggles-to-keep-food-safe/PiDOXu-yFU6OgReB69ubww.cspx

New USDA study identifies local gaps in meat processing. The U.S. Department of Agriculture has released a preliminary study revealing existing gaps within regional food systems regarding the availability of slaughter facilities for small meat and poultry producers. The study, by USDA's Food Safety and Inspection Service, is a first attempt to identify areas in the U.S. where small livestock and poultry producers are concentrated, but may not have access to a nearby slaughter facility. An interesting feature of the study are maps that provide a county-by-county view of the continental United States, indicating the concentration of small farms raising cattle, hogs and pigs, and chickens. In addition, the maps also note the location of nearby state slaughter facilities, and small and very small federal slaughter establishments. Source: http://www.farmforum.net/node/21469

Government Sector (including Schools and Universities)

(District of Columbia) **Official flushes 'anthrax' down Capitol toilet with hundreds of tourists nearby.** Lawmakers June 9 expressed outrage that a supervisor with the Capitol Visitor Center (CVC) in Washington D.C. flushed a white powder from a plastic bag labeled "Anthrax" down a toilet at the Capitol while hundreds of tourists milled around nearby. After being notified by a visitor assistant that the powder-filled bag was in the CVC's Exhibition Hall, an operational supervisor allegedly

retrieved a pair of plastic gloves and brought it to a nearby bathroom and flushed its contents down a toilet. About an hour later, Capitol Police were notified. The hazardous devices unit found no traces of harmful biological components, such as anthrax spores, during an inspection June 5 that covered the restroom, the route the supervisor allegedly took there and the area where the bag was found. The Hill is not naming the operational supervisor who flushed the substance because the identity of the employee has not been confirmed by an on-the-record source. Source: http://thehill.com/homenews/house/102213-guide-flushes-anthrax-down-capitol-toilet-with-tourists-nearby

Cyberattacks still top security priority. USIS released a study that identified key issues facing government and industry security personnel and identified a key issue in terms of security vendor structure and organization. USIS surveyed more than 250 government and industry leaders in the safety, security, and law enforcement market. Survey respondents were asked to rate the top threats to U.S. national security. Cyberattacks ranked the highest, followed by terrorist activity. Tied for third place were insider threats and information security breaches. The survey also asked participants about their most important security business imperatives. Cybersecurity topped this list at 84 percent, followed by physical security and infrastructure protection at 74 percent, and then risk management planning at 73 percent. A key finding of the survey showed that organizations with one vendor in place (rather than multiple vendors) to manage, install, maintain, and monitor security did a better job at securing the organization's infrastructure. The survey revealed that 62 percent of those with one vendor in place were able to use the data available to monitor and manage threats "very well." The majority (74 percent) of those who had one vendor in place to manage the installation, maintenance and monitoring of security said that they monitored security either "very well" or "perfectly." Source: http://www.net-security.org/secworld.php?id=9386

(North Carolina) **Explosive device found at Fort Bragg gate.** An entrance to Fort Bragg in North Carolina was shut down for a few hours Tuesday after a vehicle tried to enter the base with an explosive in its trunk. Officers detained a contractor who works on base around 10 a.m. as he was going through the All-American access checkpoint. Fort Bragg officials said guards at one of the gates found a"bazooka type round" in a car. The 772nd Explosive Ordinance Disposal Team was called in to remove the vehicle and dispose of the explosive. The access control point was re-opened two hours later. The contractor was not taken into custody. Source: http://www.wect.com/Global/story.asp?S=12615387

Satellite launch begins new era of explosion monitoring. The National Nuclear Security Administration (NNSA) has announced the deployment of a satellite that heralds the beginning of a new era of space-based nuclear-explosion monitoring. On May 27, the U.S. Air Force successfully launched the first I-I-F series of satellites, carrying improved nuclear detonation detection instruments built by Sandia National Labs and Los Alamos National Laboratory for the NNSA. The Principal Assistant Deputy Administrator said the deployment of the new instruments will significantly improve the agency's ability to detect atmospheric, or space-based, nuclear explosions and verify compliance with nuclear test ban treaties. The sensors are being integrated on to Air Force GPS satellites, thus the entire planet is monitored continuously for tell-tale signs of treaty violation. Source: http://www.federalnewsradio.com/?nid=178&sid=1974873

U.S. intelligence analyst arrested in Wikileaks video probe. Federal officials have arrested an Army intelligence analyst who boasted of giving classified U.S. combat video and hundreds of thousands of classified State Department records to whistleblower site Wikileaks, Wired.com reports. The suspect, a 22 year-old army specialist from Potomac, Maryland, was stationed at Forward Operating Base Hammer, 40 miles east of Baghdad, where he was arrested nearly two weeks ago by the Army's Criminal Investigation Division. A family member said he is being held in custody in Kuwait, and has not been formally charged. The suspect was turned in late last month by a former computer hacker with whom he spoke online. In the course of their chats, the suspect took credit for leaking a headline-making video of a helicopter attack that Wikileaks posted online in April. The video showed a deadly 2007 U.S. helicopter air strike in Baghdad that claimed the lives of several innocent civilians. He said he also leaked three other items to Wikileaks: a separate video showing the notorious 2009 Garani air strike in Afghanistan that Wikileaks has previously acknowledged is in its possession; a classified Army document evaluating Wikileaks as a security threat, which the site posted in March; and a previously unreported breach consisting of 260,000 classified U.S. diplomatic cables that the suspect described as exposing "almost criminal political back dealings." Source: http://www.wired.com/threatlevel/2010/06/leak/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+wired/index+(Wired:+Index+3+(Top+Stories+2))

Information Technology and Telecommunications

Tool automates social engineering in man-in-the-middle attack. French researchers have developed an automated social engineering tool that uses a man-in-the middle attack and strikes up online conversations with potential victims. The proof-of-concept (PoC) HoneyBot poses convincingly as a real human in Internet Relay Chats (IRC) and Instant Messaging (IM) sessions. It lets an attacker glean personal and other valuable information from victims via these chats, or lure them into clicking on malicious links. The researchers had plenty of success in their tests: They were able to get users to click onto malicious links sent via their chat messages 76 percent of the time. The researchers who created the PoC — all of Institut EURECOM in France — are also working on taking their creation a step further to automate social engineering attacks on social networks. The researchers originally wrote their HoneyBot PoC tool as a way to demonstrate large-scale automated social engineering attacks. While spammers typically send IM messages that attempt to lure users to click on their malicious links, these attacks are often fairly conspicuous and obvious to the would-be victim. Such an attack could occur via an online shopping Web site or bank site that contains an embedded chat window, the researchers said. An attacker then could set up a phishing site and wage a man-in-the-middle attack on the chat window. Source: http://www.darkreading.com/insiderthreat/security/privacy/showArticle.jhtml?articleID=225600304

Drive-by download attack disguised by Canadian Pharmacy Web site. Red Condor issued a June 10 warning of a new, sophisticated e-mail malware threat that spoofs YouTube and uses a redirect on a compromised Web site to a common Canadian Pharmacy Web site to distribute malicious PDFs via drive-by download. The pharmacy page is actually a red herring that has distracted many security researchers from the true motive of these campaigns, a stealth drive-by download. With a single click, users can infect their computers. The malware, which as of the morning of June 9 had not been detected by any anti-virus engines, comes as a malicious PDF download. Red Condor has captured 10 versions of the malicious PDF, which likely exploits vulnerabilities in Adobe Acrobat. The campaign appears to be part of a much larger attack first detected by the company several weeks ago and has

also recently spoofed Facebook and Twitter, among other popular brands. As unsuspecting users wait for what they believe is a YouTube or Twitter friend request, a greeting card, or even a Facebook log-in page to load, their browsers download and execute the malicious code, and then the Canadian Pharmacy page appears. "The amount of effort behind these new campaigns is not commensurate with the typical Canadian Pharmacy spam campaigns that we have seen in the past," said the CEO of Red Condor. Source: http://www.net-security.org/malware_news.php?id=1372

New zero-day vulnerability in Microsoft Windows XP and 2003 discovered. Microsoft has warned of a new zero-day vulnerability for Windows XP/2003, just two days after its monthly Patch Tuesday. The vulnerability is in the Windows Help and Support Center component and is accessed through the protocol handler "hcp://." A researcher who discovered and detailed the vulnerability claimed on his Twitter feed that "the risk is too high to keep this one quiet." He said that upon successful exploitation, a remote attacker is able to execute arbitrary commands with the privileges of the current user. He said: "Some minor modifications will be required to target other configurations, this is simply an attempt to demonstrate the problem. I'm sure the smart guys at Metasploit will work on designing reliable attacks, as security professionals require these to do their jobs." In terms of affected software, the researcher said: "At least Microsoft Windows XP and Windows Server 2003 are affected. The attack is enhanced against IE8 and other major browsers if Windows Media Player is available, but an installation is still vulnerable without it. Machines running version of IE less than 8 are, as usual, in even more trouble." Source: http://www.scmagazineuk.com/new-zero-day-vulnerability-in-microsoft-windows-xp-and-2003-discovered/article/172078/

Researchers: Poor password practices hurt security for all. A large-scale study of password-protected Web sites revealed a lack of standards across the industry that harms end-user security, according to two researchers working at the University of Cambridge in England. In particular, the weak implementations of password-based authentication at lower-security sites compromises the protections offered at higher-security sites because individuals often re-use passwords, the two researchers asserted in a paper presented at the Workshop on the Economics of Information Security in Cambridge, Massachusetts June 7. Attackers can use low-security Web sites such as news outlets to figure out passwords associated with certain e-mail addresses, and then use those passwords to access accounts at higher-security sites such as e-commerce vendors, one of the researchers said. In an effort that the researchers said is the largest empirical investigation into password implementations to date, they collected data from 150 Web sites and found widespread "questionable design choices, inconsistencies, and indisputable mistakes," according to the researchers. The researchers seemed disinclined to blame users for re-using passwords or making them easy to guess, arguing that most users have too many online accounts to manage them all securely. The large majority — 78 percent — of sites examined failed to provide users with feedback or advice on choosing a strong password. Only five sites let the user register password hints, a strategy that encourages users to come up with stronger passwords. Just seven sites required users to mix numbers and letters, and only two demanded passwords include non-alphanumeric characters as well. Source: http://www.computerworld.com/s/article/9177780/Researchers_Poor_password_practices_hurt_security_for_all

Adobe zero-day vulnerability exploited by backdoor Trojan on a PDF file. The zero-day vulnerability on Adobe Flash, Reader, and Acrobat is being exploited by a strain of malware. A Symantec

researcher claimed that Trojan.Pidief.J, a PDF file that drops a backdoor onto the compromised computer if an affected product is installed, is a new threat to the vulnerability. He said that attacks on the vulnerability can take place by receiving an e-mail with a malicious PDF attachment or with a link to the malicious PDF file or through a Webs ite with the malicious SWF embedded in HTML code or by stumbling across a malicious PDF or SWF file when surfing the Web."We have confirmed that the attack involves Trojan.Pidief.J, which is a PDF file that drops a backdoor Trojan onto the compromised computer if an affected product is already installed," the researcher stated. Source: http://www.scmagazineuk.com/adobe-zero-day-vulnerability-exploited-by-backdoor-trojan-on-a-pdf-file/article/171911/

Researchers release point-and-click Web site exploitation tool. Researchers have released software that exposes private information and executes arbitrary code on sensitive Web sites by exploiting weaknesses in a widely used Web-development technology. Short for Padding Oracle Exploitation Tool, Poet is able to decrypt secret data encrypted by the JavaServer Faces Web development framework without knowing the secret key. Attackers can use the technique to access private customer data on Web sites operated by banks, e-commerce companies and other businesses, according to a paper released in February by two researchers. In some cases, the exploit can be used to run malicious software on the underlying server. In the software released June 7, one of the researchers exploits a well-known vulnerability in the way many Web sites encrypt text stored in cookies, hidden HTML fields and request parameters. The text is designed to help servers keep track of purchases, user preferences and other settings while at the same time ensuring account credentials and other sensitive data can't be intercepted. By modifying the encrypted information and sending it back to the server, the attackers can recover the plaintext for small chunks of the data, allowing them to access passwords and restricted parts of a Webserver. Source: http://www.theregister.co.uk/2010/06/08/padding_oracle_attack_tool/

Open-Source databases pose unique security challenges. As the growth in Web 2.0 applications spurs adoption of open-source databases within the enterprise, many organizations need to expand their security priorities to include these increasingly important data stores. While the security principles that drive proprietary database protection also apply to open-source databases, there are a few additional challenges to locking down such platforms, which include Postgres, Ingres, and MySQL. "This is a difficult problem," said the CTO and analyst at Securosis. "The reason is there is very little effort or research put into security policies for the open-source databases. Comparing Oracle to Postgres, as an example, is a little like comparing Microsoft Windows to Apple's OS: Windows may be the more secure platform now, but only a few people write exploit code for Snow Leopard. Since we don't hear about attacks that often, we assume it's more secure." The market for open-source databases was at about $850 million in 2008, according to Forrester Research, which predicted that figure to increase to $1.2 billion by the end of this year. Gartner is more conservative in its prediction for the market, expecting open-source databases to be at $1 billion by 2013. Source: http://www.darkreading.com/database_security/security/app-security/showArticle.jhtml?articleID=225400064

Update: Attackers exploit critical bug in Adobe's Flash, Reader. Adobe late Friday warned that attackers are exploiting a critical vulnerability in the company's most widely-used software: Flash Player and Adobe Reader. The zero-day vulnerability is reminiscent of one Adobe disclosed and patched in July 2009, and comes just days after the company's head of security admitted hackers

have its software in their crosshairs. Adobe said that the bug affects Flash Player 10.0.45.2, the most up-to-date version of the popular media player, as well as older editions on Windows, Macintosh, Linux and Solaris. Also vulnerable: PDF viewer Adobe Reader 9.x and PDF creation software Adobe Acrobat 9.x on Windows, Macintosh and Unix. Hackers are already exploiting the flaw. "There are reports that this vulnerability is being actively exploited in the wild against Flash Player, Reader and Acrobat," the company said in a security advisory issued around 3:30 p.m. PT Friday. Danish bug tracker Secunia rated the threat as "extremely critical," the highest ranking in its five-step scoring system. The U.S. Computer Emergency Readiness Team (US-CERT), an arm of the federal Department of Homeland Security, also posted a warning of the vulnerability. Attackers exploiting the flaw may be able to hijack the targeted computer, Adobe acknowledged. Source: http://www.computerworld.com/s/article/9177705/Update_Attackers_exploit_critical_bug_in_Adobe_s_Flash_Reader

FTC examines privacy risks of copier hard drives. The U.S. Federal Trade Commission is urging the photocopier industry to address privacy risks arising from the fact that digital copiers store thousands of documents on their internal hard drives. CBS News reported in mid-April that nearly every copier built since 2002 stores images of documents that pass through the machines. The report found sensitive health and law-enforcement information on copiers ready to be resold. Xerox Corp. offers customers the option of removing the hard drives from copiers that they are about to dispose of or turn in after a lease, a company spokesman said. The copy machine maker also offers a free image-overwrite option that destroys information stored on many models' hard drives, he said. Source: http://www.computerworld.com/s/article/350037/FTC_Examines_Privacy_Risks_of_Photocopiers

National Monuments and Icons

(Arkansas) **14 dead in Arkansas flooding.** At least 14 people died at an Arkansas campground after heavy rain and flash flooding, and many more could be trapped in the area, state authorities said. Arkansas's governor said there is word from the Red Cross that there could have been as many as 300 people in the rugged Albert Pike campground area of western Arkansas, but he said there is no registration that would show the precise number. A state police spokesman who confirmed the death toll, said a search is on for people still trapped in the area, a relatively remote and rural region where cell phone service could be spotty. . Source: http://www.cnn.com/2010/US/06/11/arkansas.campground.deaths/index.html?hpt=T1

(Tennessee) **Bill would add 20,000 acres to Cherokee National Forest.** Tennessee's U.S. senators June 9 introduced the Tennessee Wilderness Act of 2010 that would designate six different areas totaling 19,556 acres as wilderness in the Cherokee National Forest. The areas were recommended for wilderness status by the U.S. Forest Service (USFS) in the development of its comprehensive 2004 forest plan, and have been managed as Wilderness Study Areas (WSAs) since that time. The bill specifically creates one new wilderness area, and expands the boundaries of five separate existing wilderness areas already within the Cherokee National Forest. Since these areas are owned entirely by the USFS and are being managed as WSAs currently, this bill will have no effect on privately owned lands and will cause no change in access for the public. Source: http://www.thedailytimes.com/article/20100610/NEWS/100609926

Postal and Shipping

Seattle man charged in suspicious mailings to Republican senator. A Seattle man is facing federal charges following allegations that he sent letters laced with white powder to a South Carolina senator. In charging documents, federal prosecutors claim the man mailed a letter containing white powder, staples, and paper clips to the office of the senator in an attempt to cause damage. Federal investigators contend the man admitted to the mailings, saying he was angered by "propaganda" sent to him by the Senator's office. Writing the court, a Seattle-based postal inspector said the U.S. Postal Inspection Service launched an investigation following a May 8 incident in which a postal employee's face was dusted with the white powder while handling the suspect's letter to the Senator. Postal inspectors opened the letter two days later. "A business reply letter was found addressed to [the] Senator from [the accused] with a handwritten message stating, 'I hope you choke on your own excrement such as this,' " the postal inspector told the court. "The envelope also contained staples, paper clips, a prong fastener, and loose white powder." The powder was later determined to be baking soda. The inspector added that the accused claimed to be unaware of the 2001 anthrax mailings, which killed five people and injured 17 when letters laced with the powdered biological agent were sent to various locations. Records filed with the U.S. District Court for Western Washington show the man was arrested Wednesday and released on bond later in the day. He has pleaded not guilty to a single count of attempted destruction of government property and is expected to return to court June 30. Source:
http://www.seattlepi.com/local/421560_DeMint10.html?source=mypi

(Florida) **Bioterror scare in Florida.** Jacksonville, Florida emergency workers responded to a bioterror threat Monday after a man opened an envelope that contained a suspicious substance, according to the Florida Times-Union. An unidentified Mandarin man was taken to Memorial Hospital in Jacksonville Monday for observation after he opened an envelope containing a suspicious substance at his Sugar Mill apartment on Crown Point Road. The incident also scrambled the Jacksonville fire department's hazardous-material team to test, then seal up the unknown material for further testing as police cordoned off the neighborhood for hours. Fire department spokesman Tom Francis said the man opened the letter just before 1 p.m. and felt nauseous. Until more thorough tests are done at the Duval County Health Department, it won't be clear what was mailed to the man, said an official with the homeland security division of the sheriff's office. "They will do preliminary checks to see if there are any biological threat, radiological threat, or any chemical threat," the official said. Source:
http://www.bioprepwatch.com/news/213337-bioterror-scare-in-florida

(Nebraska) **'Destructive device' used in mailbox explosion.** Gage County sheriff's deputies responded to a mailbox explosion early Monday morning at 45330 U.S. Highway 77 near Wymore, Nebraska. According to police reports, the reporting party, told deputies that between 1:30 and 1:45 a.m. Monday, her son heard a loud explosion outside their residence and observed a small grass fire by the mailbox across the highway. The woman said they later found their mailbox to be damaged and observed an explosive device in the mailbox that appeared to have been detonated. Deputies searched the area around the mailbox and found a 12-inch rubber tube that had been modified into an explosive device. After investigating the device, it was determined that it had been detonated and no longer was a threat. The Gage County chief deputy said the device was poorly constructed. "It wasn't a pipe bomb, it was a destructive device," the chief deputy said. "It was poorly constructed

and it actually just deflagrated, it didn't explode. It just burned at a rapid rate." Source: http://www.beatricedailysun.com/news/local/article_82cc125e-7355-11df-b113-001cc4c03286.html

(North Carolina) **Police investigate suspicious package at immigration office.** Authorities are investigating a suspicious package at the Citizenship and Immigration Services on Roycroft Drive off of South Miami Boulevard in the Research Triangle Park in Durham, North Carolina. According to police, three female employees who work in the mailroom complained of itchy eyes and nausea. A manager notified police of the situation. The employees were decontaminated before being taken to the hospital. Authorities evacuated everyone from the building as a precaution, and a haz-mat team began decontaminating the interior just after 10 a.m. Police said the package arrived Monday. It had an oily substance on its exterior and was isolated to the mailroom. The building where the package was delivered is also known as the Application Support Center and offers fingerprinting services needed after filing immigration papers. The only other ACS office is in Charlotte. Police have not made a connection between this incident and Monday's incident at the capitol building, but they are investigating the possibility of a link. Monday evening, authorities evacuated the State Capitol after a staffer in the governor's office opened a letter that contained white powder. The powder tested negative for hazardous materials, according to preliminary results from the North Carolina Division of Public Health. Source: http://abclocal.go.com/wtvd/story?section=news/local&id=7484916

(Ohio) **Threatening note, suspicious powder found at statehouse.** Investigators responded to a report of a suspicious package containing white powder at an Ohio government building shortly before 5 p.m. Friday. A package was discovered shortly after 3:30 p.m. at the statehouse loading dock, a 10TV worker reported. The package was addressed to the Ohio Senate and contained a suspicious powder. The package came from Illinois, the journalist reported. The powder was later determined to be baby powder, but because the package did contain a threatening note, investigators said they would turn the information over to the FBI. Officials described the letter as "hate mail," the journalist reported. The statehouse was not evacuated and no injuries were reported. As a precaution, the statehouse's ventilation system was shut off during the investigation. Source: http://www.10tv.com/live/content/local/stories/2010/06/04/story-columbus-statehouse-suspicious-package.html?sid=102

Public Health

(New Hampshire) Skin cancer rates soar in N.H. A new report shows women in New Hampshire are diagnosed with the deadliest form of skin cancer at a higher rate than their peers elsewhere. The Department of Health and Human services study found the melanoma rate for women ages 15 to 39 — was 38 percent higher than the same group nationally. Officials aren't sure why the numbers are so much higher in the Granite State and say the difference is too big to be explained by better detection. Source: http://www.wcax.com/Global/story.asp?S=12633567

Transportation

Senate eyes event data recorder rule. The Senate is considering a mandate that would require event data recorders to be installed in medium- and heavy-duty trucks, according to the American Trucking Associations' (ATA) Truckline newsletter. The possible rule is part of the larger Motor Vehicle Safety Act, which is intended to address safety in the passenger vehicle market. However, a Senator from

New Mexico has introduced an amendment to the legislation extending the requirement to trucks. In response, the ATA said it is supportive of the use of event data recorders as long as they are used to make vehicle engineering safety improvements. The group wants to avoid the use of the data in post-crash litigation. ATA has been working with the Society of Automotive Engineers to produce a recommended practice for heavy vehicle electronic data recorders. Source: http://www.truckinginfo.com/news/news-detail.asp?news_id=70681

FAA issues tire-safety rules. Prompted by landing-gear tire failures that led to a fatal 2008 plane crash, U.S. regulators have established new rules to ensure proper tire pressure on more than 200 Learjet business aircraft. Slated to be issued Tuesday by the Federal Aviation Administration (FAA), the safety directive requires U.S. operators to conduct more-frequent landing gear inspections of Learjet 60 models, which are especially susceptible to takeoff hazards from under-inflated tires. The FAA said such stepped-up scrutiny is intended to prevent tires on 240 of those models flown by U.S. operators from coming apart during takeoffs, "which could result in failures of the braking and the thrust reverser systems" and potential loss of airplane control. Operators now will have to check tire pressure on Learjet 60 models every four days. But the FAA rejected recommendations by federal crash investigators to order such checks daily. The agency also said it won't impose enhanced tire-inspection requirements on additional Learjet models, or on other types of business aircraft. Source: http://online.wsj.com/article/SB10001424052748703302604575294072660453954.html?mod=WSJ_latestheadlines

FMCSA to propose easing of supporting documents for EOBR users. Under a pending Federal Motor Carrier Safety Administration proposal, carriers that use electronic recorders will get a break on the list of documents required to prove they are in compliance with the hours of service rules. The agency is asking for comments on a plan to drop a half-dozen documents from its required list altogether, and many more for carriers that are using qualified electronic recorders to track driver hours. The policy change is the first step toward an anticipated revision of the new electronic recorder requirement. That rule, which takes effect June 2012, says carriers that violate hours of service rules 10 percent of the time, based on single compliance review, must use electronic onboard recorders to track driver hours. Later this year the agency is planning to propose a rule that will require many more carriers to use EOBRs. This policy change is in anticipation of that move. One part of the policy change affects all carriers. The agency said it will no longer consider these items to be supporting documents: driver call-in records; international registration plan receipts; international fuel tax agreement receipts; trip permits; cash advance receipts; and driver fax reports. These documents are simply not used regularly by enforcement officials, the agency explained. Specifically, the carrier will not have to keep: gate record receipts; weigh/scale tickets; port of entry receipts; delivery receipts; toll receipts; agricultural inspection reports; over/short and damage reports; driver and vehicle examination reports; traffic citations; overweight/oversize reports and citations; carrier pros; credit card receipts; border crossing reports; customs declarations; and telephone billing statements. Carriers that take advantage of this policy would not be able to challenge the accuracy of their electronic tracking records. Source: http://www.truckinginfo.com/news/news-detail.asp?news_id=70630

Water and Dams

(Wyoming) **Water levels fluctuate in swollen Wyo. rivers.** The water in one river in flood-drenched west-central Wyoming has started dropping, but others continue to rise — and more moisture is on the way. The National Weather Service extended the flood warning for rain and melting snow in central Wyoming through noon Friday. A significant rise in the middle fork of the Popo Agie River is expected later Thursday. The Wyoming National Guard is making its largest in-state activation since 2000 in response to the flooding. Rapidly melting mountain snowpack and rain have pushed rivers in the area to record or near-record levels, washing away bridges, flooding homes and curtailing drinking water supplies. Flooding also is occurring in south-central Wyoming, but sandbagging efforts have proved largely successful in Saratoga and other small communities threatened. Fremont County has already been declared a disaster area by the state because of widespread flooding from raging rivers carrying away trees and debris the size of small cars. Flooding had disabled the water treatment plant at Ethete, a community of about 1,500 people on the Wind River Indian Reservation, but the plant was working by Wednesday night and the water was drinkable. Water was shipped in earlier in the day. Residents in Lander were under water restrictions that included no watering of lawns and voluntary limits on dish washing because flooding had reduced the capacity at Lander's water treatment plant. The water was still safe to drink. About 220 members of the Wyoming National Guard are helping stuff sand bags, keep watch over evacuated homes and help respond to needs in Fremont County where rivers overflowing with quickly melting mountain snows have washed out bridges and flooded homes. About a 22-square-mile area of Fremont County with about 2,100 homes was flooded or threatened by flooding. The homes are in Lander and Riverton, and in other widely dispersed rural areas. Source: http://www.gillettenewsrecord.com/articles/2010/06/10/news/state_news/news28.txt

EPA's new Clean Watersheds Needs Survey demonstrates growing Infrastructure funding gap. The U.S. Environmental Protection Agency (EPA) this week released its Clean Watersheds Needs Survey (CWNS) report to Congress which documents a total need of $298.1 billion as of January 1, 2008, which further emphasizes the growing need for water infrastructure funding currently facing our nation. The CWNS report is available approximately every four years and provides a complete analysis of wastewater and stormwater treatment and collection needs for the next 20 years. The CWNS report includes the following investment needs: publicly owned wastewater pipes and treatment facilities ($192.2 billion); combined sewer overflow (CSO) correction ($63.6 billion); and stormwater management ($42.3 billion). This funding shortfall represents a 17 percent increase since the 2004 CWNS report, noting that something must be done now to reverse this disturbing trend. As exemplified by the 2008 CWNS report, the clean water community is increasingly facing financial capability and affordability challenges in the face of one of the most devastating economic downturns since the Great Depression. Source: http://www.watertechonline.com/news.asp?N_ID=74245

Manufacturing facilities release pharmaceuticals to the environment. Pharmaceutical manufacturing facilities can ba significant source of pharmaceuticals to surface waters, according to a new study bythe U.S. Geological Survey (USGS) conducted in cooperation with the State of New York. Outflow from two wastewater treatment plants in New York that receive more than 20 percent of their wastewater from pharmaceutical facilities had concentrations pharmaceuticals that were 10 to

1,000 times higher than outflows from 24 plants nationwide that do not receive wastewater from pharmaceutical manufacturers. “This the first study in the U.S. to identify pharmaceutical manufacturing facilities as a significant source of pharmaceuticals to the environment,” said the USGS associate director for water. While pharmaceutical concentrations were significantly lower in receiving streams, measurable concentrations were detected as far as 20 miles downstream. By contrast, outflow from the wastewater treatment plants that do not receive wastewater from pharmaceutical manufacturing facilities had concentrations that rarely exceeded one part per billion. For this study, USGS scientists collected outflow samples periodically from 2004 to 2009 from three New York wastewater treatment plants, two of which receive more than 20 percent of their wastewater from pharmaceutical manufacturing facilities. USGS also collected samples from 2006-200from 23 selected wastewater treatment plants across the nation that do not receive wastewater from pharmaceutical manufacturing facilities. All of the samples were analyzed for seven pharmaceuticals, including opioids and muscle relaxants, representing some of the most frequently prescribed medications in the U.S. Source: http://www.enewspf.com/index.php/latest-news/science-a-environmental/16754-manufacturing-facilities-release-pharmaceuticals-to-the-environment

(South Carolina) **Copper thieves shut down Lyman wastewater operation.** A copper theft temporarily shut down the South Carolina town of Lyman’s Wastewater Plant, but officials restored service by early Saturday evening and said the theft caused no public health threat. The supervisor of the Lyman Wastewater Division said the Groce Road plant was hit sometime between 4 p.m. Friday and 9 a.m. Saturday. He said the plant was able to obtain materials to replace copper wires that went from motor starters to switch boxes. Platforms that were no longer in service also were taken. He did not yet have a cost estimate for the missing items and damages. The plant processes residential and industrial wastewater for the town and some surrounding areas prior to its discharge in the Tyger River. The copper theft shut down the pumping, and all of the untreated water stayed in its proper place until the plant resumed pumping operations. He said the problem caused by the theft was “more of a nuisance.” Lyman police responded to the plant about 9 a.m., when an employee discovered and reported the theft. The Spartanburg County Sheriff’s Office assisting the Lyman Police Department with the investigation. Source: http://www.goupstate.com/article/20100606/ARTICLES/6061025/1083/ARTICLES?tle=Copper-thieves-shut-down-Lyman-wastewater-operation

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(In ND only); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**


NDDES
Homeland Security
State Radio
NORTH DAKOTA
STATE PATROL
NORTH DAKOTA
STRENGTH FROM THE SOIL
NATIONAL GUARD